UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* The person of TAYDE Katy Zepeda Mendez, born 06/15/1978, for the cellular telephone assigned call number 414-797-5116 (TARGET DEVICE) and the TARGET DEVICE	)	Case No. 25-947M(NJ)

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Eastern District of Wisconsin *(identify the person or describe the property to be searched and give its location)*:

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before 6/12/2025 *(not to exceed 14 days)*

☑ in the daytime 6:00 a.m. to 10:00 p.m. ❒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Honorable Nancy Joseph.
(United States Magistrate Judge)

❒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

❒ for _____ days *(not to exceed 30)* ❒ until, the facts justifying, the later specific date of _____.

Date and time issued: 5/30/2025 9:30 a.m.

Nancy Joseph
Judge's signature

City and state: Milwaukee, WI

Honorable Nancy Joseph, U.S. Magistrate Judge
Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

Person to be searched

The person of TAYDE Katy Zepeda Mendez, born 06/15/1978, for the cellular telephone assigned call number 414-797-5116 (TARGET DEVICE).

Device to be searched

The TARGET DEVICE

ATTACHMENT B

Evidence to be seized

1. All records and information on the TARGET DEVICE, described in Attachment A, that relate to violations of Title 18, U.S.C., § 1343 (Wire Fraud) and Title 26, U.S.C., § 7206(2) (aiding or assisting in the preparation of false or fraudulent tax returns) and involve TAYDE Katy Zepeda Mendez since January 1, 2019, including:

a. All records, information, and communications relating to the logistics of aiding and/or assisting in the preparation of false or fraudulent tax returns;

b. Records, information, and communications with current and former tax preparation clients;

c. Records and information relating to the identity or locations of the suspects, associates, co-conspirators, and clients;

d. IRS publications, regulations, and/or copies of IRS forms and documents, extracts from the Internal Revenue Code, and any correspondence relating to IRS forms, Internal Revenue Statutes or regulations and tax schedules;

e. Documents or materials related to training in tax law and/or the preparation of tax returns, including but not limited to training manuals, examples, templates, and correspondence in electronic, video, or paper formats;

f. Originals or copies of federal and state income tax returns, income tax forms and tax-return-preparation software, whether blank or completed, and whether filed with the IRS or not;

g. Tax return schedules and forms, tax return worksheets, and other related supporting documents, including but not limited to attachments, questionnaires, work papers, notes, telephone messages, electronic filing documents, correspondence or documents from refund recipients and/or other tax preparers, and documents relating to deductions and credits claimed on any federal income tax returns;

h. Financial records or information relating to the preparation of client tax returns, including records documenting or purporting to document the receipt of income by a taxpayer or the expenditure of money by a taxpayer, including Forms W-2, employment records, receipts, accounting books and records, bank account records, brokerage account records, checks, deposit slips, withdrawal slips, currency exchange records, money orders, cashier's checks, images of checks, check stubs, earnings statements, and school or day care records or bills;

i. Financial records or information relating to the receipt and/or status of tax refunds, tax refund loans, or the expenditure of proceeds of such tax refunds or tax refund loans, including but not limited to receipts, bank account records, brokerage account records, U.S. Treasury checks, deposit slips, withdrawal slips, currency exchange records, money orders, cashier's checks, credit card

applications and records, debit card and prepaid credit card applications and records, Refund Anticipation Loan (RAL) applications, RAL checks, and invoices;

j. Personal identification documents, records, or information;

k. Records identifying the taxpayers for whom tax returns have been prepared including client listings, correspondence, telephone books, appointment records, calendars, diaries, notes and other identifying information of the clients;

l. Invoices, receipts, ledgers, schedules, and other records relating to tax consulting or tax preparation fees charged and payments received;

m. Financial records related to Amalia Zepeda Peralta, Tayde Katy Zepeda Mendez, and/or any variations of said names, including, but not limited to, bank account records, bank statements, deposit statements/slips, receipts, cash receipt books, checks, check books, canceled checks, check registers, withdrawal slips, Certificates of Deposits documents, wire transfers, cashier's checks, money orders, mutual fund and other securities' records, credit applications, loan documents, loan payments, loan statements, invoices and/or bills;

n. Records and information relating to the e-mail accounts:

    i. documentos.express@yahoo.com;

    ii. zepedatayde@yahoo.com;

iii. peraltaamlia@yahoo.com;

2. Evidence of user attribution showing who used or owned TARGET DEVICE at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

During the execution of the search of the person described in Attachment A, law enforcement personnel are authorized to obtain from TAYDE Katy Zepeda Mendez the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint, facial characteristics, or iris display) necessary to unlock TARGET DEVICE requiring such biometric access subject to seizure pursuant to this warrant for which law enforcement has reasonable suspicion that the aforementioned person's physical biometric characteristics will unlock TARGET DEVICE, to include pressing fingers or thumbs against and/or putting a face before the sensor, or any other security feature requiring biometric recognition, for the purpose of attempting to unlock TARGET DEVICE's security features in order to search the contents as authorized by this warrant.

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

The person of TAYDE Katy Zepeda Mendez, born 06/15/1978, for the cellular telephone assigned call number 414-797-5116 (TARGET DEVICE) and the TARGET DEVICE

Case No. 25-947M(NJ)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the Eastern District of Wisconsin, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Title 18 U.S.C. § 1343	Wire Fraud
Title 26 U.S.C. § 7206(2)	Aiding or Assisting in the preparation of false or fraudulent tax returns

The application is based on these facts:

See Attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Digitally signed by Nummerdor Jared D
Date: 2025.05.29 15:32:49 -05'00'

Applicant's signature

Jared Nummerdor, Special Agent - IRS-CI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 5/30/2025

Judge's signature

City and state: Milwaukee, WI

Honorable Nancy Joseph, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Jared Nummerdor, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the search of Tayde Katy Zepeda Mendez (TAYDE) for the cellular telephone assigned call number 414-797-5116 (TARGET DEVICE), as described in Attachment A. I further request that the contemplated search warrant authorize the search of TARGET DEVICE for evidence more fully described in Attachment B.

2. I am a Special Agent with the Internal Revenue Service – Criminal Investigation (IRS-CI) and have been since December 4, 2023. I am currently assigned to the Chicago Field Office and conduct investigations in the Eastern District of Wisconsin. I have completed the Criminal Investigator Training Program and the Special Agent Basic Training for IRS-CI at the Federal Law Enforcement Training Center in Glynco, GA. I have a bachelor's degree from Lakeland University located in Sheboygan, Wisconsin where I majored in accounting with an emphasis in fraud and forensics, and I minored in criminal justice.

3. Through my specialized training I have learned, among other things, financial investigative techniques used to carry out my responsibilities of conducting criminal investigations relating to violations of the Internal Revenue Code (Title 26, United States Code), the Money Laundering Control Act (Title 18, United States Code), the Bank Secrecy Act (Title

31, United States Code), and other related offenses. My training and experience include the execution of search warrants.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, witnesses, and agencies. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on the facts disclosed in this affidavit, there is probable cause to believe that TAYDE and others have committed violations of Title 18 U.S.C. § 1343 (wire fraud) and Title 26 U.S.C. § 7206(2) (aiding or assisting in the preparation of false or fraudulent tax returns) (the "SUBJECT OFFENSES") and that evidence and instrumentalities of such crimes is likely to be found on TARGET DEVICE, as described in Attachment B. As a result, there is probable cause to search TAYDE's person, further described in Attachment A, for TARGET DEVICE, described in Attachment B, and to further search TARGET DEVICE, described in Attachment B, for evidence of the SUBJECT OFFENSES.

BACKGROUND RELATING TO IRS REGULATIONS AND PROVISIONS

6. Every person who earns United States (U.S.) source income is required to pay taxes. U.S. citizens are required to pay taxes on worldwide income from whatever source derived. The IRS typically treats any individual living in the U.S., either legally or illegally, as a

resident alien who is taxed on worldwide income and required to file an income tax return just like any U.S. citizen.

7. Every person who files a U.S. income tax return must provide a taxpayer identification number when the person files a return. For American citizens or resident aliens who entered the United States legally, this would typically be a Social Security Number (SSN). However, individuals, such as resident aliens and non-resident aliens who are not eligible for an SSN, must apply for an Individual Taxpayer Identification Number (ITIN). An ITIN is for tax use only and does not change a taxpayer's immigration status or his/her legal right to work in the U.S. An ITIN can be distinguished from an SSN because the first number is a nine, has a range of numbers from "50" to "65", "70" to "88", "90" to 92" and "94" to "99" for the fourth and fifth digits and is formatted like an SSN (i.e. 9XX-7X-XXXX). Only resident aliens and nonresident aliens (having earned income in the United States and therefore required to file a federal individual income tax return) who do not have, and are not eligible for, a social security number may apply for an ITIN.

8. In order to obtain an ITIN, a taxpayer must submit to the IRS an Application for IRS Individual Taxpayer Identification Number, Form W-7, and an original valid U.S. Federal Income Tax Return or documentation explaining the exception to the tax return requirement. In addition, the following documents of personal identifying information (PII) must be submitted:

a. An original passport or;

b. A combination of two or more Personally Identifying Information ("PII") documents that show the taxpayer's name and photograph (with the exception of children under the age of 14). These documents include: United States Citizenship and Immigration Services photo ID; national ID card; Visa issued by the US; US or Foreign Driver's License; US or Foreign Military Card; foreign voter ID card; birth certificate; school records (if under the age of 14); medical records (if under the age of 6); and/or some other identifying document. In lieu of originals, the taxpayer may provide copies that are certified by the issuing agency.

9. If IRS accepts the Application for Individual Taxpayer Identification number, IRS will process the tax return, issue each person on the tax return an ITIN, and mail each person listed on the tax return IRS Notice CP565. IRS Notice CP565 is letter alerting the applicant that their application was accepted and providing the applicant with a specifically assigned ITIN. IRS Notice CP565 also lists instructions for the proper use of an ITIN.

SOURCES OF INFORMATION

10. The information set forth in this affidavit is based on my personal knowledge and investigation, information that I received from other law enforcement officers, and information I have learned from the other sources specifically discussed herein. I believe these sources of information to be credible and reliable based on the corroboration of the information and my experience with these matters. The information in this affidavit does not include all of my

knowledge and investigation into this case. These facts are presented for the sole purpose of establishing probable cause in support of the application for a search warrant.

11. Based on my training, experience, and feedback from other experienced law enforcement officers, I am aware that:

a. Tax return preparer fraud schemes normally involve multiple false tax returns that appear to have been prepared by the same individual. The tax returns normally share similar tax return characteristics that establish a pattern of fraud.

b. Tax return preparer fraud schemes often involve the electronic filing (e-filing) of false tax returns using false Form(s) W-2, Wage and Tax Statement, with inflated wages and inflated federal and state income tax withholdings to obtain a larger income tax refund. In actuality, the individual listed as the employee on each Form W-2 did not earn the wages from the employer listed and did not have the amount of income tax withholdings.

c. Individuals who engage in an ITIN refund scheme for a given year will frequently do the same scheme, or a similar scheme, in the following year.

d. Tax return preparers involved in the preparation of false tax returns normally maintain records of their activity, such as copies of tax returns, records of scheme participants including addresses, SSNs, and ITINs, supporting schedules and

forms, and supporting worksheets. I know that these records are often stored on computer media, including the computers, cellular telephones, and other media used to file tax returns electronically. I know that many individuals retain possession of computers, cellular telephones, and other media for long periods of time, and individuals involved in the preparation and electronic filing of tax returns maintain the records for long periods of time. This is normally done so that the same information can be used for subsequent filing seasons.

e. Return Preparers filing ITIN scheme returns do not list any identifying information in the paid preparer section of the tax returns they prepare, making it difficult for authorities to trace returns back to that particular tax preparer.

f. Individuals engaging in illegal activity (including the illegal activity described in this affidavit) often use cellular telephones because of their ability to make phone calls, send text messages and other messages (iMessages and WhatsApp messages), send and receive emails, and access other communication applications, such as Facebook Messenger.

g. Individuals engaged in a refund fraud scheme, such as ITIN return schemes, coordinate appointments, receiving information to put on the tax returns from clients, with clients using cellular telephones, via phone calls, text messages, other messages, or instant messaging apps.

h. Cellular telephones, such as smart phones, connect to the internet and have location data, which can provide evidence of a crime in an ITIN return scheme if the location data from the phone overlaps with the locations from where the fraudulent tax returns were filed or where the fraudulent tax returns were prepared.

PROBABLE CAUSE

12. I am currently investigating an allegation that TAYDE and Amalia Zepeda Peralta (Peralta), TAYDE's sister, aided or assisted taxpayers by preparing and filing false or fraudulent federal tax returns with the IRS. These tax returns allegedly report false Forms W-2 with inflated federal income tax withholdings in order to obtain refunds to which the taxpayers were not entitled. This investigation encompasses the 2019 through 2024 tax years.

ITIN Scheme Noticed in TAC

13. On August 22, 2024, an Individual Taxpayer Advisory Specialist (ITAS) from the Milwaukee, WI Taxpayer Assistance Center (TAC) was interviewed. The ITAS believed they had spotted a possible Individual Taxpayer Identification Number (ITIN) scheme going through the Milwaukee, WI TAC. They noticed a trend of individuals going into the TAC under the

Taxpayer Protection Program (TPP)[1] to verify each individuals' identities. The individuals all had ITINs and Forms 1040, U.S. Individual Income Tax Returns (Form 1040), for the 2021, 2022, and 2023 tax years.

14. The ITAS described the individuals as being Hispanic, bringing in three tax returns, having ITINs, most having Forms W-2, from the same few employers, and at the beginning, all having the same female interpreter. Each Form 1040 had Forms W-2 attached showing approximately $50,000 or more in gross wages and federal income tax withholdings of approximately $14,000 to $16,000. Each Form 1040 resulted in federal income tax refunds equaling approximately $10,000 or more.

15. Once the ITAS notice the trend, they asked the interpreter what her name was. The female interpreter responded saying her name was "Martha." After asking for her name, the ITAS has not seen the female interpreter in the Milwaukee, WI TAC.

Referral to SDC & SDC's Report

[1] The TPP is a program in which the IRS proactively identifies and prevents the processing of tax returns that may involve identity theft. If an individual's return is flagged by the TPP, the individual can go to the TAC and verify their identity. Once their identity is verified the return will be processed.

16. I reviewed the information provided by the ITAS and referred the information to the IRS-CI Scheme Development Center (SDC). The SDC assigned an analyst to investigate the data, and the analyst wrote up a report, dated 09/25/2024.

17. The SDC analyst identified approximately 1,013 tax returns linked to the ITIN scheme matching information collected by the IRS. These returns were linked via Device ID: C03037D0211B69D065FE31DDA66FF091A94061AC and the following emails:

a. documentos.express@yahoo.com

b. zepedatayde@yahoo.com

c. sasomaricela@yahoo.com

d. peraltaamalia@yahoo.com

e. 2adriancervantes@gmail.com

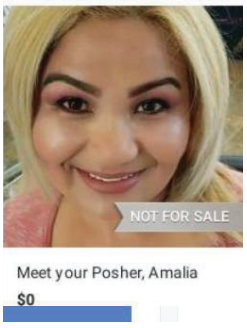
18. A summary of the returns the SDC analyst found follows:

Processing Year	Total Returns	Refund Claimed	Refund Claimed	Refunds Issued[1]
2024*	279	275	$2,867,178.00	$2,240,065.00
2023	224	222	$1,570,315.00	$1,446,969.00
2022	188	183	$1,308,345.00	$1,080,490.00
2021	203	200	$1,133,531.00	$915,735.00
2020	119	116	$718,892.00	$603,607.00
Total	1013	996	$7,598,261.00	$6,286,866.00
2024		98.6%		
2023		99.1%		
2022		97.3%		
2021		98.5%		
2020		97.5%		
Total		98.3%		

Current processing year returns as of 09/16/2024.

[1]*The refunds Issued figures represent the dollar amount of refunds issued by the government. They may not be the same as the Refunds Claimed amount due to questionable refunds held, audits, adjustments, penalties, and interest. It is possible that a portion of the refunds are comprised of a portion of legitimately owed refunds. To accurately assess the Harm to the Government additional investigative actions are needed.*

19. The SDC analyst also conducted Open-Source Intelligence Research (OSINT) for the emails indicated above. A search of the email, documentos.express@yahoo.com, developed associated accounts with Twitter, username express2511, and with Poshmark, username aperalta81. Poshmark is an online shopping marketplace where buyers and sellers connect with each other to sell different fashion items. The username aperalta81 on Poshmark was link to Amalia Zepeda (Peralta) with the following photo:



20. I showed this picture to the Milwaukee, WI TAC ITAS, and the ITAS stated the female in the picture was Martha, the interpreter that was initially coming into the TAC with the individuals identified in the ITIN scheme.

Landmark Credit Union

21. On February 19, 2025, I talked with a Landmark Credit Union (LCU) Investigator. The investigator stated that four individuals with Nicaraguan passports were brought into LCU by Adelina Garcia Velazquez (Velazquez) to set up bank accounts and deposit federal income tax refund checks. Three of the individuals were brought to LCU on January 3, 2025, and the other individual was brought to LCU in December 2024. During one of the interactions, Velazquez told a LCU associate that the individuals got their tax returns prepared by Amalia Zepeda (Peralta) at 5512 W. North Ave., Apt 270, Milwaukee, WI.

22. I researched the federal tax returns of the four individuals who went into LCU. The federal tax returns matched the same characteristics of the ITIN scheme.

23. On March 18, 2025, I received documentation from a BSA Team Lead at LCU. Per LCU, on March 6, 2025, an EDD (Enhance Due Diligence) Analyst with LCU conducted a member outreach with TAYDE. To my understanding a member outreach is when an LCU associate calls the bank customer. Per LCU documents, the EDD Analyst spoke with TAYDE, who confirmed that she is a tax preparer, and she is working with her sister, who has a tax

license. It goes on to say TAYDE states that her clients are paying her via Zelle[2]. TAYDE stated that she charges $500 for a business and $320 for a personal tax return. TAYDE admitted that she and her sister were unable to get business accounts and that is why the payer-to-payer credits are coming into her personal bank account. TAYDE also stated she sells clothing and electronics to her customers and that is why the credits are higher than her stated fees. TAYDE stated she splits the money with her sister by allowing her sister to use her Landmark debit card to buy personal items and pay bills.

24. Based on my knowledge, experience, and investigation to date, I believe the sister mentioned in the conversation, between the EDD Analyst and TAYDE, is Amalia Zepeda Peralta. I believe TAYDE's use of Zelle potentially indicates her use of a cellular telephone in furtherance of the ITIN scheme.

Madison TAC Interactions

25. On February 6, 2025, the manager for the Milwaukee, WI TAC informed me that the manager for the Madison, WI TAC was also having appointments matching the ITIN

---

[2] Per Zelle's Website, "Zelle® is a convenient way to send and receive money with friends, family and others you trust through your bank or credit union's mobile app or online banking. All you need is your recipient's email address or U.S. mobile number, and money will be available to use in minutes if they're already enrolled with Zelle®. Your account information and activity stay private. Zelle® is available in over 2,200 bank and credit union apps - so it's probably already in yours."

scheme. All the individuals that were going to the Madison, WI TAC had Milwaukee, WI addresses.

26. On February 24, 2025, IRS-CI Special Agents interviewed the employees of the Madison, WI TAC. The TAC employees stated they have assisted individuals to verify their identities through the Taxpayer Protection Program, so the refunds could be paid out. They believed the individuals were part of the same ITIN scheme. Each individual had an appointment and came into the TAC with manilla folders in a plastic bag. Each manilla folder had the requested refund amount written on the outside of the folder. The individuals were mostly Nicaraguan and sometimes Mexican.

27. The Madison TAC security officer cleared all the individuals coming into the TAC. When he cleared the individuals matching the ITIN scheme, they were typically carrying either a clear or black plastic bag with documents in it. The security officer noticed dollar amounts written on the manilla folders. The security officer described a day where he observed a lady sitting in the back of a black Jeep Wagoneer, Wisconsin license plate AZM3917, handing out manilla folders to the individuals in the parking lot. The individuals would then come into the TAC to get their identities verified. The lady handing out manilla folder never entered the TAC.

28. The Jeep Wagoneer with Wisconsin license plate AZM3917 is registered to Abexayda Yamilet Peralta (Abexayda), believed to be the daughter of TAYDE and niece of Peralta per social media postings by Abexayda, TAYDE, and Peralta.

29. March 11, 2025, TAYDE accompanied a potential client, matching the ITIN scheme, into the Madison, WI TAC. TAYDE acted as the interpreter for the potential client when they were verifying their identity. I believe this to be true because it was reported to me by a TAC employee and the interpreter, TAYDE, provided a Washington State identification card with her name.

Milwaukee & Madison TAC Summary

30. As of April 1, 2025, there have been 76 different individuals identified matching the ITIN Scheme who came into the Milwaukee and Madison, Wisconsin TACs or Landmark Credit Union. There was 263 tax returns filed with the IRS with the tax years 2019 through 2024. These tax returns were processed in the years 2023 through 2025. See the summaries of the returns below:

Processing/Tax Year	# of Tax Returns	Refund Claimed
2023	**12**	**$ 110,254.00**
2019	4	31762
2020	3	31132
2021	3	36117
2022	2	11243
2024	**157**	**$ 1,891,621.00**
2020	22	271921
2021	46	554356
2022	45	547351
2023	44	517993
2025	**87**	**$ 1,347,631.00**
2020	7	103089
2021	12	173270
2022	14	205585
2023	14	215389
2024	40	650298
(blank)	**7**	**$ 99,347.00**
2021	2	27359
2022	1	15013
2023	3	40711
2024	1	16264
Grand Total	**263**	**$ 3,448,853.00**

Creation Email Analysis

31. I know the IRS captures an email address associated with the creation of tax returns on tax preparation software. Based on IRS data, of the 263 returns mentioned above, there have been 21 e-filed tax returns, matching the ITIN Scheme, with the creation email, zepedatayde@yahoo.com. See the summary table below:

Associated Creation Email	# of Returns	Refund Claimed
DOCUMENTOS.EXPRESS@YAHOO.COM	27	$ 389,985.00
sandovalyahary@gmail.com	1	$ 16,805.00
ZEPEDATAYDE@YAHOO.COM	21	$ 310,119.00
(blank)	214	$ 2,731,944.00
Grand Total	**263**	**$ 3,448,853.00**

32. Based on my knowledge, experience, and investigation to date, I believe the email address, zepedatayde@yahoo.com, is TAYDE's email address. This is based on the email address being used on TAYDE's We Energies and Charter Communication profiles. More information from We Energies and Charter Communication is explained below.

Forms W-2 Analysis

33. I am aware that the IRS receives two different copies of Forms W-2. One of the copies is received from the taxpayers when it is attached with their Forms 1040. The second copy is received from the Social Security Administration (SSA). Employers are responsible for sending a copy of the employees Forms W-2 to the SSA and the SSA shares them with the IRS. These two copies of the Forms W-2 should match.

34. Of the above mentioned 263 tax returns identified, there were 150 returns where I can see the attached Form W-2. Using IRS databases, I compared the attached Forms W-2 with Employer's Forms W-2 shared to the IRS by the SSA. See the below summary:

Description	# of Returns	Refund Claimed
a - No W2 matching SSN, ITIN, or Name	88	$ 1,191,258.00
b - W2 from employer with matching SSN/ITIN and name. 1040 W2 has inflated wages and withholdings.	9	$ 108,108.00
c - W2 from employer with matching name and different SSN/ITIN. 1040 W2 has inflated wages and withholdings.	2	$ 29,404.00
d - W2 from different employer with matching SSN/ITIN and name. 1040 W2 has inflated wages and withholdings.	20	$ 274,374.00
e - W2 from different employer with matching SSN/ITIN and name. 1040 W2 has deflated wages and inflated withholdings.	1	$ 13,799.00
f - W2 from employer with matching SSN and different name.	3	$ 42,582.00
g - W2 from different employer with matching SSN/ITIN and different name.	27	$ 397,362.00
Grand Total	**150**	**$ 2,056,887.00**

35. I have identified seven different ways the Forms W-2 are fraudulent and/or false. The descriptions in the above table have the following explanations:

a. 88 tax returns had a Form W-2 attached that had no matching Form W-2 sent in by any employer. This means there was no Form W-2 that matched either the individuals name, SSN, or ITIN associated with the tax return. Due to no Forms W-2 matching, I could not compare the wages or federal income tax withholdings. With no actual Form W-2, the tax returns filed with these non-existent Forms W-2 are fraudulent. For this section, SSN or ITIN will be identified as Taxpayer Identification Number (TIN).

b. Nine tax returns had a Form W-2 attached that had a name and TIN that matched a Form W-2 sent in by the actual employer on the Form W-2 attached to the tax returns. The wages and federal income tax withholdings on the Form W-2 attached to the tax return were inflated compared to the Form W-2 sent in by the employer. This inflation causes the tax returns to be fraudulent.

c. Two tax returns had a Form W-2 attached that had a name that matched a Form W-2 sent in by the actual employer on the Form W-2 attached to the tax returns, but the TIN was not matching. The wages and federal income tax withholdings on the Form W-2 attached to the tax return were inflated compared to the Form W-2 sent in by the employer. This inflation causes the tax returns to be fraudulent.

d. 20 tax returns had a Form W-2 attached that had a name and TIN that matched a Form W-2 sent in by a different employer then what was on the Form W-2

attached to the tax return. The wages and federal income tax withholdings on the Form W-2 attached to the tax return were inflated compared to the Form W-2 sent in by the different employer. This inflation causes the tax returns to be fraudulent.

e. There was one tax return that had a Form W-2 attached to it that had a name and TIN that matched a Form W-2 sent in by a different employer than what was on the Form W-2 attached to the tax return. The Form W-2 attached to the tax return had deflated wages compared to the Form W-2 sent in by the different employer, but it had federal income tax withholdings inflated compared to the Form W-2 sent in by the different employer. The inflation of federal income tax withholdings caused this tax return to be fraudulent.

f. Three tax returns had a Form W-2 attached that had a TIN matching a Form W-2 sent in by the actual employer on the Form W-2 attached to the tax returns, but the name of the taxpayer did not match. Due to the name not matching, I did not compare the wages or federal income tax withholdings. The name identifying someone else causes cause the Form W-2 attached to the tax return to be false and/or fraudulent.

g. 27 tax returns had a Form W-2 attached that had a TIN matching a Form W-2 sent in by a different employer than what was on the Form W-2 attached to the tax returns, but the name of the taxpayer did not match. Due to the name not

matching, I did not compare the wages or federal income tax withholdings. The name identifying someone else, would cause the Form W-2 attached to the tax return to be false and/or fraudulent.

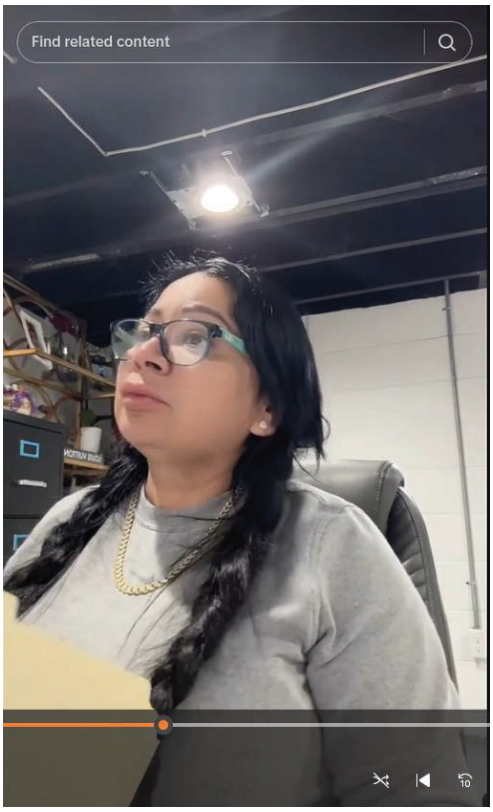
3222 South 24th Street, Milwaukee Drive-bys & Surveillance

36. On March 11, 2025, and March 14, 2025, a Black Jeep Wagoneer with Wisconsin State license plate AZM3917, registered to Abexayda, was spotted parked in the alleyway garage of 3222 South 24th Street, Milwaukee, WI 53215. Per We Energies' records, TAYDE is the name on the We Energies' account for the provided utilities. This Wagoneer is the same vehicle spotted at the Madison WI TAC where a female was spotted handing out manilla folders to potential clients of the ITIN scheme. Based on my knowledge, experience, and investigation to date, the Wagoneer is primarily used by TAYDE.

Tayde's Social Media Posts

37. Through OSINT research, it was discovered TAYDE has a TikTok account with the username Kathy.zepeda50 and a name of Kathy Zepeda. I noticed two specific videos that show characteristics of the ITIN scheme described in this affidavit.

38. On approximately April 23, 2025, TAYDE posted a video in what appears to be a basement office where she is holding a manila folder. There is also a black filing cabinet in the background. See the following screen capture:



39. On approximately April 25, 2025, TAYDE posted a video in what appears to be the same basement office where she is holding a manila folder. There is also a shelf in the background with a stack of manila folders and sleaves of paper. See the following screen capture:

UC Phone Call

40. On March 10, 2025, an IRS-CI undercover agent (UC) attempted to call a phone number, 414-524-9949, later confirmed to have Peralta as the subscriber from Verizon. A female

answered and the UC attempted to make an appointment with the female, but the female indicated that she only takes new clients by referral. She told the UC to have whoever referred the UC to call her first. Based on my training, experience, and the investigation to date, I believe that this is proof Peralta is engaging in illegal activity because if she is a small tax preparer, who is legitimately preparing taxes, it would be unusual to turn down business like this.

We Energies Records

41. Per We Energies' records, the contract information for TAYDE included the cellular telephone number, 414-797-5116 (TARGET DEVICE). Based on my knowledge, experience, and investigation to date, I believe this number to be TAYDE's primary phone number used.

42. Per We Energies' records, the contact information for TAYDE also included an email address, Zepedatayde@yahoo.com. Per IRS records, this email address has been linked to the fraudulent returns matching the ITIN scheme.

Verizon Records

43. Per Verizon's records, since January 18, 2024, the phone number, 414-524-9949, subscriber is Peralta. Per Verizon's call detail records, on March 10, 2025, the phone number, 414-524-9949, received a phone call from the UC phone number.

44. Per Verizon's call logs for Peralta's phone number, 414-524-9949, the TARGET DEVICE was called by Peralta 555 times between March 16, 2024, and March 9, 2025. Peralta was called from TARGET DEVICE 662 times between March 14, 2024, and March 10, 2025. This totals 1,217 phone conversations between the dates of March 14, 2024, and March 10, 2025. Between March 14, 2024, and March 10, 2025, there are approximately 361 days, so this would average approximately 3.37, or 3-4, phone calls per day between TAYDE and Peralta.

45. Based on my knowledge, experience, and investigation to date, I believe this shows TAYDE and Peralta were in communication during the time period of the illegal ITIN scheme. I believe this shows communication to facilitate the ITIN scheme described in this affidavit.

Charter Communication IP Addresses

46. Between the dates of March 19, 2024, through January 21, 2025, the following ten IP Addresses have been linked to tax returns matching the ITIN scheme filed with the IRS:

a. 2603:6000:A800:6F5:14AA:634A:C1A2:E1CC

b. 2603:6000:A800:6F5:3887:A2CF:CE07:2DAA

c. 2603:6000:A800:6F5:5CC7:E4E6:6A54:5F16

d. 2603:6000:A800:6F5:99A0:3B75:249C:C4AB

e. 2603:6000:A800:6F5:DCC7:2FF9:6756:713A

f. 2603:6000:A800:6F5:FCBB:961B:5E7E:CAA6

g. 2603:6000:A8F0:2160:79C8:2437:1195:F81C

h. 2603:6000:A8F0:2160:8429:ACC2:771B:2D45

i. 2603:6000:A8F0:2160:9972:EBDA:D8C0:A271

j. 2603:6000:A8F0:2160:B151:906D:2281:C1D0

47. Per Charter Communication records, the above IP Addresses were assigned to TAYDE as the subscriber. The service address for TAYDE's subscriber account for the above IP addresses was 3606 South 22nd Street, Milwaukee, WI 53221. This address is a previous address of TAYDE, per the above We Energies records.

48. On February 10, 2025, there was one Form 1040 matching the ITIN scheme was filed with the IRS from IP address 2603:6000:A7F0:5BB0:5AE:B043:6D94:7E94. Per Charter Communication records, this IP Address was assigned to TAYDE as the subscriber. The service address for TAYDE's subscriber account for this IP Address was 3222 South 24th Street, Milwaukee, WI 53215.

49. Per Charter Communication records, the above 11 IP Addresses have the "user name or features" of ZEPEDATAYDE@YAHOO.COM.

50. Based on my knowledge, experience, and investigation to date, I believe the TARGET DEVICE connects to the internet service provided by Charter Communication. TAYDE has posted various TikTok videos from what appears to be a cellular telephone in the 3222 South 24th Street, Milwaukee, WI 53215. I believe there is probable cause to believe that searching the TARGET DEVICE will reveal location evidence to prove TAYDE's location at the time the tax returns were filed with the IRS via the above IP Addresses.

Trash Pull - TARGET LOCATION #2

51. On April 11, 2025, your affiant and another IRS-CI Special Agent conducted a trash pull at the location associated with TAYDE, 3222 South 24th Street, Milwaukee, WI 53215. The trash was located outside the detached garage located in the alleyway where the garbage truck picks up the trash. The trash bin was located in the same spot reflected in the image, taken on April 10, 2025, below:

52. The items found in the trash included, a brown paper bag from Starbucks with "Tayde Z." wrote on the outside, multiple receipts with Tayde's name, two empty 100 count boxes of 3-tab file folders (manilla folders), shredded pieces of paper that appear to be tax documents, and shredded pieces of manilla folders. See the following images:

TECHNICAL TERMS

53. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address

books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This

removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a

memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

50. Based on my training, experience, and research, and from consulting the manufacturer's advertisements and product technical specifications available online, I believe that the TARGET DEVICE has the capability to allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

54. Based on my training, experience, and research, and from consulting the manufacturer's advertisements and product technical specifications available online, I believe that the TARGET DEVICE has the capability to allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

55. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

56. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the TARGET DEVICE was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on TARGET DEVICE because:

a. Data on the electronic device can provide evidence of a file that was once on the electronic device but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on an electronic device that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on an electronic device is evidence may depend on other information stored on the electronic device and the application of knowledge about how an electronic device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how an electronic device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on an electronic device.

57. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the subject devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose

many parts of the devices to human inspection in order to determine whether that part constitutes evidence described by the warrant.

58. *Manner of execution.* Because this warrant seeks permission to forensically examine devices that will, after their seizure, be in law enforcement's possession, I submit there is reasonable cause for the Court to authorize that the forensic examination portion of the warrant at any time in the day or night.

59. I know from my training and experience, as well as publicly available materials, that encryption systems for mobile phones and other electronic devices are becoming ever more widespread. Such encryption systems protect the contents of these devices from unauthorized access by users and render these contents unreadable to anyone who does not have the device's password. As device encryption becomes more commonplace, the encryption systems implemented by device manufacturers are becoming more robust, with few—if any—workarounds available to law enforcement investigators.

60. I also know that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize. Therefore, I request that this warrant permit law enforcement agents to

obtain from TAYDE the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock the TARGET DEVICE.

61. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

62. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the frontfacing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers (such as Apple's "Face ID") have different names but operate similarly to Trusted Face.

63. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

64. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

65. As discussed in this Affidavit, your Affiant has reason to believe that the TARGET DEVICE is subject to search and seizure pursuant to the applied-for warrant. The passcode or password that would unlock the TARGET DEVICE are currently not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data

contained within the TARGET DEVICE, making the use of biometric features necessary to the execution of the search authorized by this warrant.

66. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period. For example, certain Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time. Due to the foregoing, if law enforcement personnel encounter the TARGET DEVICE that is subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to obtain from TAYDE the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock the TARGET DEVICE including to (1) press or swipe the fingers (including thumbs) of the aforementioned person to the fingerprint scanner of the TARGET DEVICE; (2) hold the

TARGET DEVICE in front of the face of the aforementioned person to activate the facial recognition feature; and/or (3) hold the TARGET DEVICE in front of the face of the aforementioned person to activate the iris recognition feature, for the purpose of attempting to unlock the TARGET DEVICE in order to search the contents as authorized by this warrant.

CONCLUSION

67. I submit that this affidavit supports probable cause for a warrant to search TAYDE's person, further described in Attachment A, for the TARGET DEVICE, described in Attachments A, and to further search the TARGET DEVICE for evidence of the SUBJECT OFFENSES.

ATTACHMENT A

Person to be searched

The person of TAYDE Katy Zepeda Mendez, born 06/15/1978, for the cellular telephone assigned call number 414-797-5116 (TARGET DEVICE).

Device to be searched

The TARGET DEVICE

ATTACHMENT B

Evidence to be seized

1. All records and information on the TARGET DEVICE, described in Attachment A, that relate to violations of Title 18, U.S.C., § 1343 (Wire Fraud) and Title 26, U.S.C., § 7206(2) (aiding or assisting in the preparation of false or fraudulent tax returns) and involve TAYDE Katy Zepeda Mendez since January 1, 2019, including:

a. All records, information, and communications relating to the logistics of aiding and/or assisting in the preparation of false or fraudulent tax returns;

b. Records, information, and communications with current and former tax preparation clients;

c. Records and information relating to the identity or locations of the suspects, associates, co-conspirators, and clients;

d. IRS publications, regulations, and/or copies of IRS forms and documents, extracts from the Internal Revenue Code, and any correspondence relating to IRS forms, Internal Revenue Statutes or regulations and tax schedules;

e. Documents or materials related to training in tax law and/or the preparation of tax returns, including but not limited to training manuals, examples, templates, and correspondence in electronic, video, or paper formats;

f. Originals or copies of federal and state income tax returns, income tax forms and tax-return-preparation software, whether blank or completed, and whether filed with the IRS or not;

g. Tax return schedules and forms, tax return worksheets, and other related supporting documents, including but not limited to attachments, questionnaires, work papers, notes, telephone messages, electronic filing documents, correspondence or documents from refund recipients and/or other tax preparers, and documents relating to deductions and credits claimed on any federal income tax returns;

h. Financial records or information relating to the preparation of client tax returns, including records documenting or purporting to document the receipt of income by a taxpayer or the expenditure of money by a taxpayer, including Forms W-2, employment records, receipts, accounting books and records, bank account records, brokerage account records, checks, deposit slips, withdrawal slips, currency exchange records, money orders, cashier's checks, images of checks, check stubs, earnings statements, and school or day care records or bills;

i. Financial records or information relating to the receipt and/or status of tax refunds, tax refund loans, or the expenditure of proceeds of such tax refunds or tax refund loans, including but not limited to receipts, bank account records, brokerage account records, U.S. Treasury checks, deposit slips, withdrawal slips, currency exchange records, money orders, cashier's checks, credit card

applications and records, debit card and prepaid credit card applications and records, Refund Anticipation Loan (RAL) applications, RAL checks, and invoices;

j. Personal identification documents, records, or information;

k. Records identifying the taxpayers for whom tax returns have been prepared including client listings, correspondence, telephone books, appointment records, calendars, diaries, notes and other identifying information of the clients;

l. Invoices, receipts, ledgers, schedules, and other records relating to tax consulting or tax preparation fees charged and payments received;

m. Financial records related to Amalia Zepeda Peralta, Tayde Katy Zepeda Mendez, and/or any variations of said names, including, but not limited to, bank account records, bank statements, deposit statements/slips, receipts, cash receipt books, checks, check books, canceled checks, check registers, withdrawal slips, Certificates of Deposits documents, wire transfers, cashier's checks, money orders, mutual fund and other securities' records, credit applications, loan documents, loan payments, loan statements, invoices and/or bills;

n. Records and information relating to the e-mail accounts:

    i. documentos.express@yahoo.com;

    ii. zepedatayde@yahoo.com;

iii. peraltaamlia@yahoo.com;

2. Evidence of user attribution showing who used or owned TARGET DEVICE at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

During the execution of the search of the person described in Attachment A, law enforcement personnel are authorized to obtain from TAYDE Katy Zepeda Mendez the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint, facial characteristics, or iris display) necessary to unlock TARGET DEVICE requiring such biometric access subject to seizure pursuant to this warrant for which law enforcement has reasonable suspicion that the aforementioned person's physical biometric characteristics will unlock TARGET DEVICE, to include pressing fingers or thumbs against and/or putting a face before the sensor, or any other security feature requiring biometric recognition, for the purpose of attempting to unlock TARGET DEVICE's security features in order to search the contents as authorized by this warrant.